(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **07264668 A**

(43) Date of publication of application: **13 . 10 . 95**

(51) Int. Cl **H04Q 7/38**
H04L 9/06
H04L 9/14
H04Q 7/34

(21) Application number: **06071252**

(22) Date of filing: **17 . 03 . 94**

(71) Applicant: **KOKUSAI DENSHIN DENWA CO LTD <KDD>**

(72) Inventor: **OHASHI MASAYOSHI**
TAKEUCHI YOSHIO
SUZUKI TOSHINORI
YAMAGUCHI AKIRA
SAKAI SEIICHIRO
MIZUNO TOSHIO

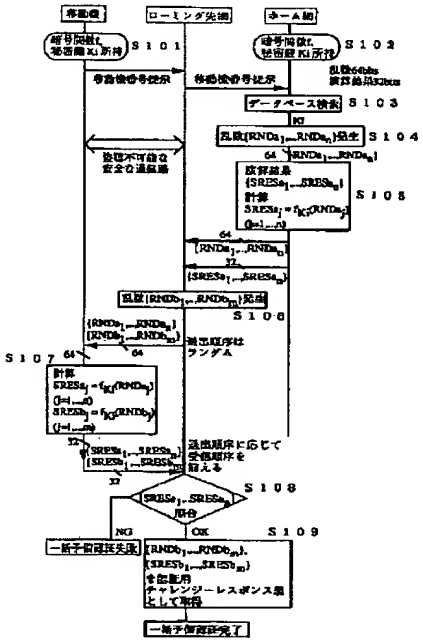
(54) **AUTHENTICATING METHOD FOR MOBILE COMMUNICATION**

(57) Abstract:

PURPOSE: To provide the authenticating method for mobile communication which can reduce the information traffic between networks by obtaining the arithmetic result of mobile equipment itself with random numbers generated in a roaming destination network.

CONSTITUTION: Separately from a normal authentication sequence, the random numbers generated in the roaming destination network is added in addition to random numbers obtained by the home network, the order is deranged to perform plural authentication processes, and a pair of the random numbers obtained by the home network and the arithmetic result are used for batch preliminary authentication. Then the order is deranged and a preliminary authentication sequence is performed; and the roaming destination network obtains random numbers and an arithmetic result by a preliminary authentication sequence, and saves and stores them, thereby performing authentication between plural mobile communication networks.

COPYRIGHT: (C)1995,JPO



(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号

特開平7－264668

(43)公開日　平成７年(1995)10月13日

(51)Int.Cl.[6]		識別記号	庁内整理番号	Ｆ Ｉ	技術表示箇所
Ｈ０４Ｑ	7/38				
Ｈ０４Ｌ	9/06				
	9/14				
				Ｈ０４Ｂ　7/ 26	１０９　Ｒ
				Ｈ０４Ｌ　9/ 02	Ｚ

審査請求　未請求　請求項の数１　ＦＤ　（全 ７ 頁）　最終頁に続く

(21)出願番号　特願平6－71252

(22)出願日　平成６年(1994)３月17日

(71)出願人　000001214
国際電信電話株式会社
東京都新宿区西新宿２丁目３番２号

(72)発明者　大橋　正良
東京都新宿区西新宿２丁目３番２号国際電信電話株式会社内

(72)発明者　武内　良男
東京都新宿区西新宿２丁目３番２号国際電信電話株式会社内

(72)発明者　鈴木　利則
東京都新宿区西新宿２丁目３番２号国際電信電話株式会社内

(74)代理人　弁理士　山本　恵一

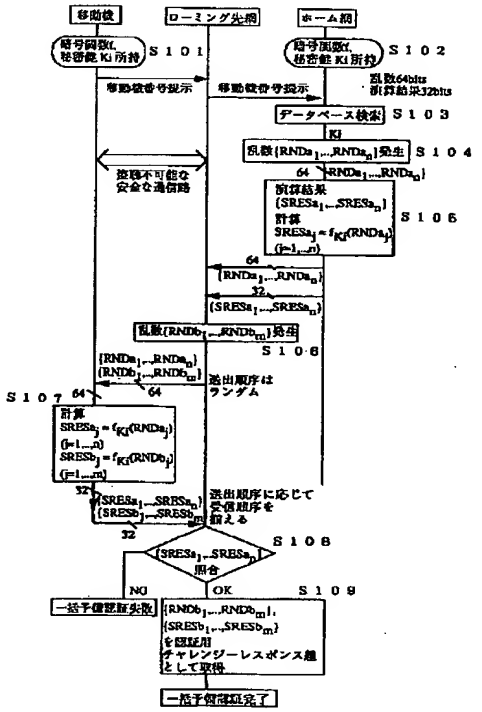
最終頁に続く

(54)【発明の名称】　移動通信認証方法

(57)【要約】

【目的】　本発明はローミング先網で作成した乱数より移動機自らの演算結果を得ることにより網間の情報転送量を削減できる移動通信認証方法を提供することを目的とする。

【構成】　本発明はこの目的を達成するために、通常の認証シーケンスと別に、ホーム網より得られた乱数の他にローミング先網で独自に発生した乱数を加え、順序を攪乱して複数の認証を行い、かつホーム網より得られた乱数と演算結果の組を一括予備認証用に用いる。そして、順序を攪乱して予備認証シーケンスを行い、ローミング先網が前記予備認証シーケンスによる乱数および演算結果を得て蓄積、記憶して、複数の移動通信網間での認証を行う。



1

【特許請求の範囲】

【請求項１】　予め同一の秘密鍵が移動機と移動機の本来属するホーム網のデータベース内に設定、記憶されると共に同一の暗号関数が移動機とホーム網に備わっており、移動機が秘密鍵を有していることを、網側から乱数を移動機に送出して移動機ではその乱数と移動機の秘密鍵を暗号関数の入力として演算を行った結果を移動通信網に返すことで証明することにより、移動機の正当性を確認する移動通信認証方法において、

複数の移動通信網が存在する条件下で、

移動機がホーム網以外の移動通信網であるローミング先網にアクセスして通信を行うために、ホーム網より乱数と当該乱数に基づく演算結果の複数の組をローミング先網に送ることによってローミング先網でホーム網と同一のアルゴリズムに従った移動機の正当性を示す認証シーケンスの場合であって、前記認証シーケンンスと別に、ホーム網より得られた乱数の他にローミング先網で独自に発生した乱数を加え、順序を攪乱して複数の認証を行い、かつホーム網より得られた乱数と演算結果の組を一括予備認証用に用い、順序を攪乱して予備認証シーケンスを行い、ローミング先網が前記予備認証シーケンスによる乱数および演算結果を得て蓄積、記憶して、複数の移動通信網間での認証を行うことを特徴とする移動通信認証方法。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は移動通信認証方法に関し、特に複数の方式が異なって存在する自動車電話等の移動通信網において、移動機が他移動網にアクセス（ローミング）して通信を行おうとする場合、その移動機が自分の本来属する移動網の正当な移動機であることを移動先の移動網が確認するための、移動通信認証方法に関する。

【０００２】

【従来の技術】移動通信網を介する通信では固定系の通信形態とは異なり、無線を介して相手移動機と接続されるため、接続される移動機が確かに所望の移動機であるかどうかが移動通信網からは明確に判明できない。

【０００３】そのため何らかの手法を用いて、移動通信網は接続移動機の正当性を確認する必要がある。この正当性確認は認証と呼ばれている。認証に当たっては、無線が傍受されやすい性質を持っている。そのために、仮に盗聴を受けたとしても、移動通信網は、後に盗聴者が不正な移動機を用い、正当な移動機のふりをして移動通信網にアクセスされない工夫が必要になる。

【０００４】このため現在のディジタル移動通信網では秘密鍵暗号方式に基づくチャレンジーレスポンス認証方式（以下ＣＲ認証方式と呼ぶ）が幅広く用いられている。

【０００５】以下、図３を用いてＣＲ認証方式を説明する。なお、ＣＲ認証方式では移動網と移動機は共通の秘密鍵暗号関数ｆを所持する。ｆは２つの変数を持ち、一つは秘密鍵Ki、一つは乱数 RNDである。秘密鍵Kiはパラメータとなるので、この関数出力をf_{Ki}(RND)と記し、その結果の値をSRESと呼ぶ。

2

【０００６】移動網は自網に所属する全ての正当な移動機の秘密鍵{Ki}を有する（Ｓ３０１）。秘密鍵は移動機すべてに異なった値が割り当てられる。正当な移動機はそれぞれ自らの秘密鍵Kiを有する（Ｓ３０２）。当該秘密鍵Kiは外部からの読み出しの攻撃に対し物理的に安全に保持されている。ＣＲ認証に際して、図示していないが移動機はまず自らの移動機番号を移動網に伝える。移動網はデータベース検索によって、対象移動機の秘密鍵Kiを得る。移動網は乱数（チャレンジ）RND を発生し（Ｓ３０３）、移動機に送出する。移動機は受け取った乱数RND と自分の秘密鍵より関数f を用いて暗号演算を行い（Ｓ３０４）、その演算結果（レスポンス）をSRESとして移動網に送り返す。移動網もKi, ｆを有するので、同じ演算を行う。その結果が移動機より送り返されてきたSRESと一致すれば、認証成功、さもなくば失敗となる（Ｓ３０５）。

【０００７】このように、ＣＲ認証方式は、移動機が正当な秘密鍵Kiを有していることを、無線区間上で直接移動網に提示することなく、RND とSRESの受け渡しのみで移動網に示すことができるため、盗聴によってもKiを知られることのない有効な方式である。

【０００８】さらに、RND は移動網によって任意に選べ、その値に応じて移動機が返す正しいSRESの値は異なるため、複数回不正な移動機が傍受を行っても、自らが正当な移動機になりすますことはできない。従って、ＣＲ認証方式は移動通信システムのセキュリティを確保する観点から非常に優れた方式の一つであるといえる。以下の説明ではすべてＣＲ認証方式を用いると仮定する。

【０００９】次に、ローミングについて説明を行う。ここで、ローミングとは移動機が自網以外の網にアクセスして通信を行う機能をいう。このとき移動機が本来属している網をホーム網、現在アクセスしている網をローミング先網と呼ぶ。ローミング時にはローミング先網は通信に先立ち、アクセスしてきた移動機がホーム網に正当に登録された移動機であるかどうかを認証する必要がある。

【００１０】しかしながら、ローミング先網は、ローミングしてきた移動機の秘密鍵を持たず、また必ずしもホーム網と同一の暗号関数f を採用しているわけではないので、自網で認証を行う時とは以下に示す場合に応じて各々異なった手順をとる必要がある。

【００１１】(1) ローミング先網がホーム網と同一の暗号関数f を有している場合

この場合には、次の二通りの方法がある。

(a) ホーム網が、対象となる移動機の秘密鍵Kiをローミ

ング先網に渡す。
(b) ホーム網が、対象となる移動機の秘密鍵Kiを用いて認証に必要なチャレンジーレスポンスの組（以下ＣＲ組と呼ぶ）{RND, SRES} を生成し、ローミング先網に渡す。
【００１２】この動作を図４に示す。同図(a) はホーム網が秘密鍵をローミング先網に渡す場合である。移動機とホーム網は暗号関数ｆと秘密鍵Kiを所持し（Ｓ４０１，Ｓ４０３）、ローミング先網は暗号関数ｆを所持している（Ｓ４０２）。移動機がローミング先網にアクセスするとローミング先網はホーム網に移動機番号を提示し、ホーム網では提示された当該移動機番号に基づいてデータベース検索を行い該当する移動機の所持する秘密鍵Kiがローミング先網へ送り返される（Ｓ４０５）。このように(a) の場合は簡便であるが、ホーム網のセキュリティの要である秘密鍵Kiをローミング網に渡すため、システムの安全性に問題がある。
【００１３】同図(b) はホーム網が対象となる移動機の秘密鍵Kiを用いて認証に必要なＣＲ組{RND, SRES} を生成してローミング先網に渡す場合である。この場合において、移動機とホーム網のみが暗号関数f と秘密鍵Kiを所持している（Ｓ４１１，Ｓ４１２）。移動機がローミング先網にアクセスするとローミング先網はホーム網に移動機番号を提示し、ホーム網では提示された当該移動機番号に基づいてデータベース検索を行う（Ｓ４１３）。そして、ホーム網では乱数$\{RND_1, \cdots, RND_N\}$を発生し（Ｓ４１４）、当該乱数と自網で所持していた秘密鍵Kiより暗号関数fを用いて暗号演算を行い、その演算結果$\{SRES_1, \cdots, SRES_n\}$ と乱数$\{RND_1, \cdots, RND_N\}$ をローミング先網へ送り返す（Ｓ４１５，Ｓ４１６）。このように(b) の場合は認証に必要な回数だけのＣＲ組をホーム網からローミング先網に転送せねばならないため転送情報量が増大する問題は存在するが、Kiが網間上の信号で直接露呈しないため、セキュリティ上安全な方式である。通常は初めてローミングを行う際に、ローミング先網はホーム網に複数のＣＲ組を要求して取得し、その後は認証ごとにホーム網に問い合わせることなく、取得セットからＣＲ組を順次使用する。ＣＲ組を全部使いきった時点でローミング先網は、再度ホーム網に新たにＣＲ組を要求して取得する。
【００１４】(2) ローミング網がホーム網と同一の暗号関数f を有していない場合
この場合には、上記(a) は適用できず上記(b) を適用せざるを得ない。但し、両網の認証方式において乱数と演算結果のビット長は一致している必要がある。ヨーロッパにおける標準のディジタル移動通信方式GSM (Global System for Mo-bile communication) では本方式が採用されている。
【００１５】
【発明が解決しようとする課題】従来の方式における上記のように(b) のＣＲの組を渡す方式は、各網の暗号関数ｆの一致を必要としない優れた方式である。しかしながら、このような従来の方式は、ホーム網からローミング先網に送出すべき情報量が増大する問題を有している。またローミング先網では、独自に決定した乱数を用いて認証を行うことができない。
【００１６】本発明はこれらの問題点を解決するためのもので、ローミング先網で作成した乱数より移動機自らの演算結果を得ることにより網間の情報転送量を削減できる移動通信認証方法を提供することを目的とする。
【００１７】
【課題を解決するための手段】本発明は上記問題点を解決するために、予め同一の秘密鍵が移動機と移動機の本来属するホーム網のデータベース内に設定、記憶されると共に同一の暗号関数が移動機とホーム網に備わっており、移動機が秘密鍵を有していることを、網側から乱数を移動機に送出して移動機ではその乱数と移動機の秘密鍵を暗号関数の入力として演算を行った結果を移動通信網に返すことで証明することにより、移動機の正当性を確認する移動通信認証方法において、複数の移動通信網が存在する条件下で、移動機がホーム網以外の移動通信網であるローミング先網にアクセスして通信を行うために、ホーム網より乱数と当該乱数に基づく演算結果の複数の組をローミング先網に送ることによってローミング先網でホーム網と同一のアルゴリズムに従った移動機の正当性を示す認証シーケンスの場合であって、認証シーケンスと別に、ホーム網より得られた乱数の他にローミング先網で独自に発生した乱数を加え、順序を攪乱して複数の認証を行い、かつホーム網より得られた乱数と演算結果の組を一括予備認証用に用い、順序を攪乱して予備認証シーケンスを行い、ローミング先網が予備認証シーケンスによる乱数および演算結果を得て蓄積、記憶して、複数の移動通信網間での認証を行うことに特徴がある。
【００１８】
【作用】以上のような本発明によれば、ローミングを行う際に、はじめに安全な通信路を用いて一括予備認証過程を行い、本過程においてホーム網より得られた乱数、演算結果のＣＲ組を用いた認証の他に、ローミング先網で発生した独自の乱数を混在させ、順序を撹拌して認証を行うことで、移動機側には全て通常の認証と同等のプロトコルを実施しているが如くに見せながら、ローミング網は、自ら発生する乱数に対する正当な複数の演算結果を網からではなく移動機側から得て、その後のローミング網における移動機の認証に有効に用いようとするものである。
【００１９】したがって、本発明は前記問題点を解決でき、ローミング先網で作成した乱数より移動機自らの演算結果を得ることにより網間の情報転送量を削減できる移動通信認証方法を提供できる。

【００２０】

【実施例】以下、本発明の一実施例を図面に基づいて説明する。図１は本発明の実施例の動作を示すフローチャートである。同図で移動機とローミング先網間の通信路は、例えば別途有線系の通信路や、通常の通話用無線通信路に暗号化を施したような、外部からの盗聴に対して安全と考えられる通信路を仮定する。移動機とホーム網は移動機の正当性を確認するための暗号関数ｆおよび移動機の秘密鍵Kiを所持する。暗号関数ｆは乱数64ビット、演算結果32ビット長とする。（Ｓ１０１，Ｓ１０２）

【００２１】はじめに、移動機がローミング先網へ予備認証の要求を行うと、ローミング先網は移動機番号を示し、かつホーム網にＣＲ組の要求を行う。ホーム網はデータベース検索を行い、当該移動機の秘密鍵Kiを検索する（Ｓ１０３）。次いでホーム網は、ｎ個の乱数{RNDa$_1$, ･･･, RNDa$_n$}を発生し（Ｓ１０４）、これに対し、秘密鍵Kiをパラメータとして暗号演算f_{Ki}(RNDa$_j$)を行い、同じくｎ個の演算結果{SRESa$_1$, ･･･, SRESa$_n$}を生成し、ローミング先網に送出する（Ｓ１０５）。ホーム網よりＣＲ組を受領したローミング先網は、別途ｍ個の乱数{RNDb$_1$, ･･･, RNDb$_m$}を発生する（Ｓ１０６）。これを前述の{RNDa$_1$, ･･･, RNDa$_n$}と結合し、送出順序をランダム化した後、チャレンジとして移動機にシリアルまたはパラレルに送出する（図１ではパラレルに送出）。

【００２２】移動機はローミング先網より送られたｍ＋ｎ個の乱数に対して自己の有する暗号関数ならびに秘密鍵Kiを用いて、演算結果{SRES}を求め（Ｓ１０７）ローミング先網に返送する。ローミング先網は、先の送信順序に応じて受信演算結果を並べ替えることにより、{SRESa$_1$, ･･･, SRESa$_n$}, {SRESb$_1$, ･･･, SRESb$_m$}を得る。このうちホーム網から予め演算結果を得ている{SRESa$_1$, ･･･, SRESa$_n$}の照合を行い（Ｓ１０８）、照合が全てOKであればこのＣＲ組を生成した移動機は正当であるとみなし、{RNDb$_1$, ･･･, RNDb$_m$}, {SRESb$_1$, ･･･, SRESb$_m$}をKiの正当な認証用ＣＲ組として後のローミング用認証に用いる（Ｓ１０９）。照合が一つでも失敗すれば、認証失敗とみなし、{SRESb$_1$, ･･･, SRESb$_m$}を棄却する。

【００２３】移動機側では、ローミング先網から送出される乱数について、どれがRNDa$_j$(j=1, ･･･, n)でどれがRNDb$_j$(j=1, ･･･, m)であるか判別不能であるため、仮に正当な移動機が、わざとRNDa$_j$にのみ正しい演算結果を渡し、RNDb$_j$に間違った演算結果を渡そうと試みても、認証完了が極めて困難である。また不正な移動機ならば、RNDa$_j$に対して正しい結果を返せない。従って正当な移動機から認証完了時に得られるＣＲ組は、高い確率で正＊当である。

【００２４】このようにしてローミング先網は、一括予備認証過程を行い、同過程が完了後、従来通りのＣＲ認証を行う。この様子を図２に示す。

【００２５】図２に示すように、実際の移動機を通じてローミング網を介した通信を要求する本認証過程では、すでにローミング先網に予備認証の結果が蓄えられている（Ｓ２０１）ので、移動機からローミング要求に対して、ローミング先網は64ビットの任意の乱数RNDb$_j$を移動機に送出する。移動機は自らが有する暗号関数ｆならびに秘密鍵Kiを用いて演算を行い（Ｓ２０２）、その結果の32ビットをSRESb$_j$としてローミング先網に返す。ローミング先網でSRESb$_j$の照合を行い、OKならば認証完了、さもなくば認証失敗となる（Ｓ２０３）。

【００２６】但し移動機にとっては、一括予備認証過程で投げかけられた乱数が、再度本認証においても使用されるため、一括予備認証過程で盗聴が行われるならば、盗聴者は本認証の際に簡単になりすましを行うことができる。従って一括認証過程における通信路は、あくまで盗聴の心配がない安全なものでなければならない。

【００２７】なお、本実施例では簡単のため、移動機は一なる存在としたが、移動通信では暗号関数や秘密鍵などは、ICカード中に納められている場合も多く存在する。この場合には、一括予備認証にはICカードのみをたとえばローミング先網の有する専用有線端末に挿入するなどの無線区間を用いない方法で行うことにより、移動機－ローミング先網間通信路の安全性を確保することも考えられる。

【００２８】

【発明の効果】以上説明しようように、本発明によれば、ホーム網から大量のＣＲ組を得なくとも、ローミング先網で作成した乱数より、移動機自らの演算結果を得ることで所望の数のＣＲ組を得ることができ、網間の情報転送量削減につながる。また何らかの事情によりローミング先網が自ら発生した乱数を用いて移動機の認証を行いたい状況で、ローミングプロトコル上乱数がホーム網からのみ発生せねばならないときに有効である。

【図面の簡単な説明】

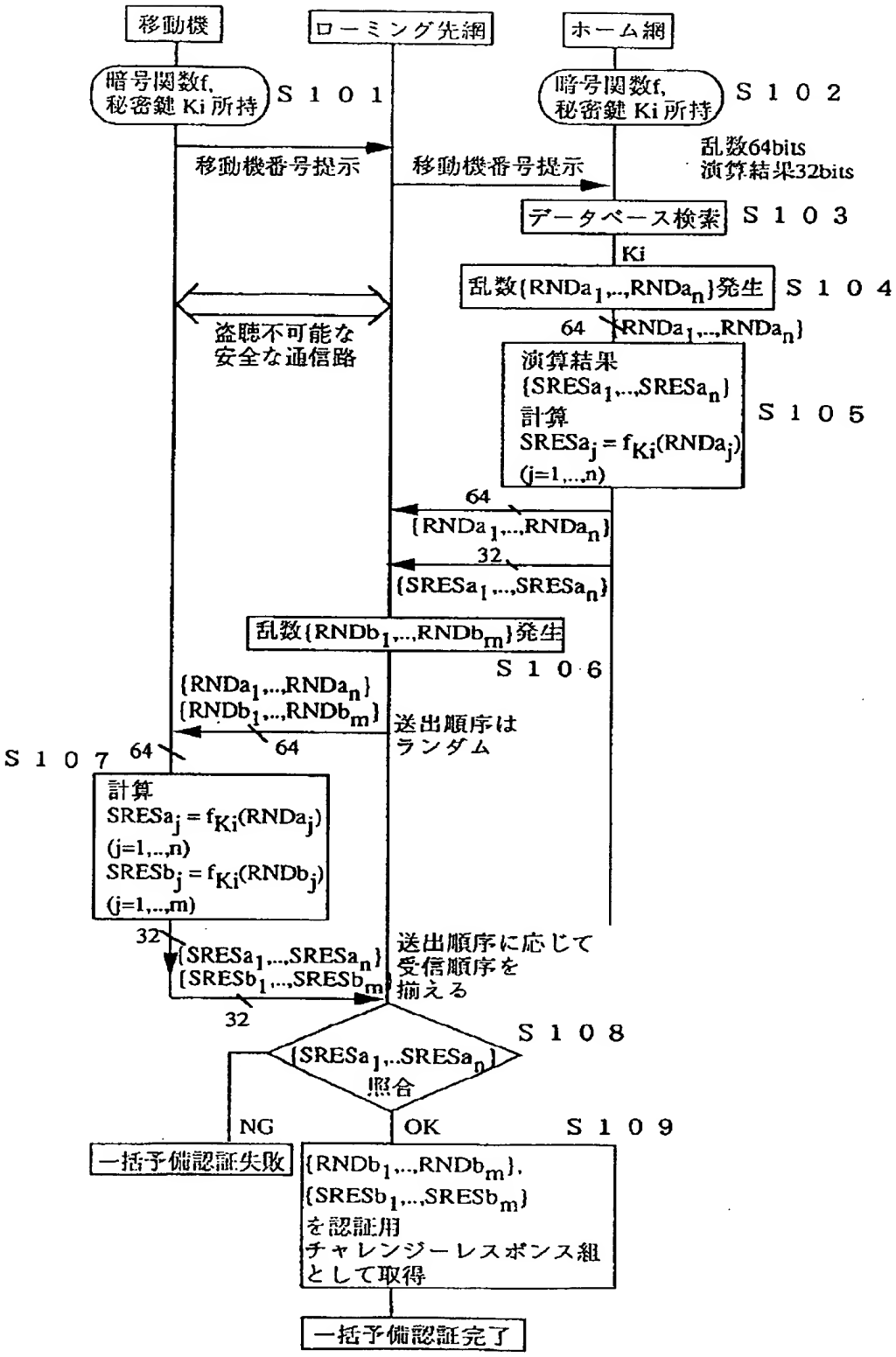
【図１】本発明の一実施例の動作における一括予備認証過程の動作を示すフローチャートである。

【図２】本実施例の動作における本認証過程の動作を示すフローチャートである。

【図３】従来のＣＲ認証方式の動作を示すフローチャートである。

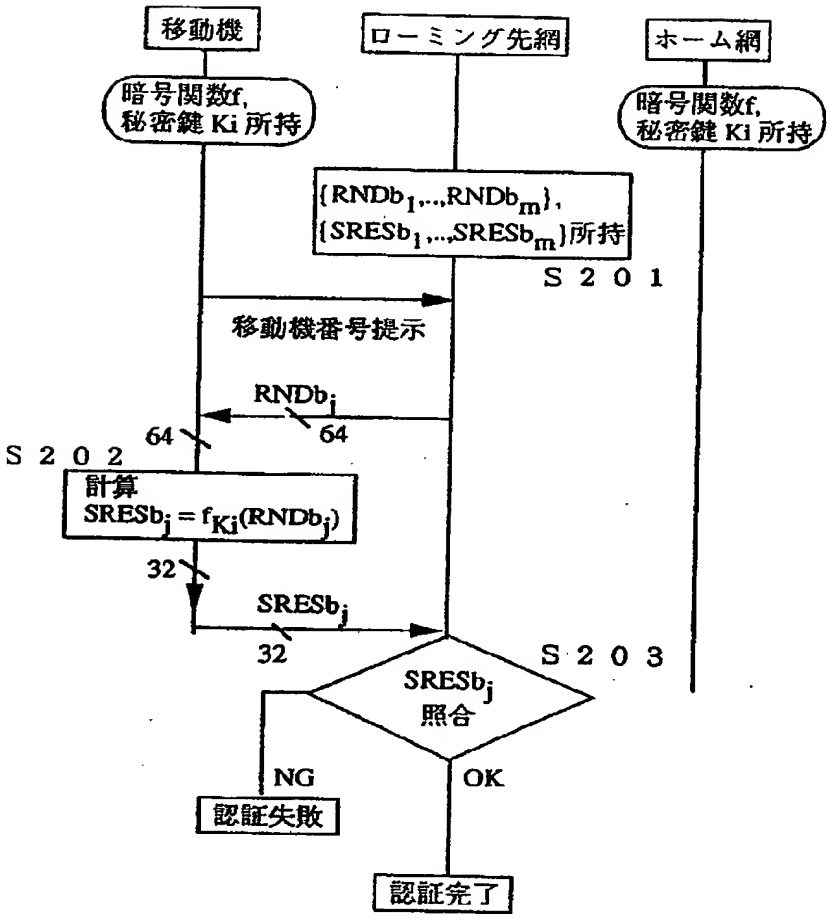
【図４】ローミング認証の原理の動作を示すフローチャートである。

【図１】

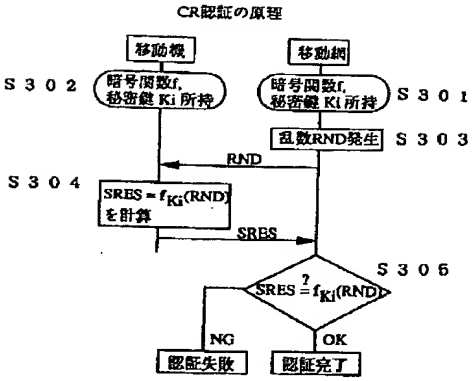

移動機
ローミング先網
ホーム網
暗号関数f,
秘密鍵 Ki 所持
Ｓ１０１
暗号関数f,
秘密鍵 Ki 所持
Ｓ１０２
移動機番号提示
移動機番号提示
乱数64bits
演算結果32bits
データベース検索
Ｓ１０３
Ki
乱数{RNDa1,..,RNDan}発生
Ｓ１０４
64
{RNDa1,...,RNDan}
盗聴不可能な
安全な通信路
演算結果
{SRESa1,..,SRESan}
計算
SRESaj = fKi(RNDaj)
(j=1,..,n)
Ｓ１０５
64
{RNDa1,...,RNDan}
32
{SRESa1,...,SRESan}
乱数{RNDb1,..,RNDbm}発生
Ｓ１０６
{RNDa1,..,RNDan}
{RNDb1,..,RNDbm}
送出順序は
ランダム
Ｓ１０７
64
64
計算
SRESaj = fKi(RNDaj)
(j=1,..,n)
SRESbj = fKi(RNDbj)
(j=1,..,m)
32
{SRESa1,...,SRESan}
{SRESb1,...,SRESbm}
送出順序に応じて
受信順序を
揃える
32
Ｓ１０８
{SRESa1,..SRESan}
照合
NG
OK
Ｓ１０９
一括予備認証失敗
{RNDb1,..,RNDbm},
{SRESb1,..,SRESbm}
を認証用
チャレンジーレスポンス組
として取得
一括予備認証完了

【図２】

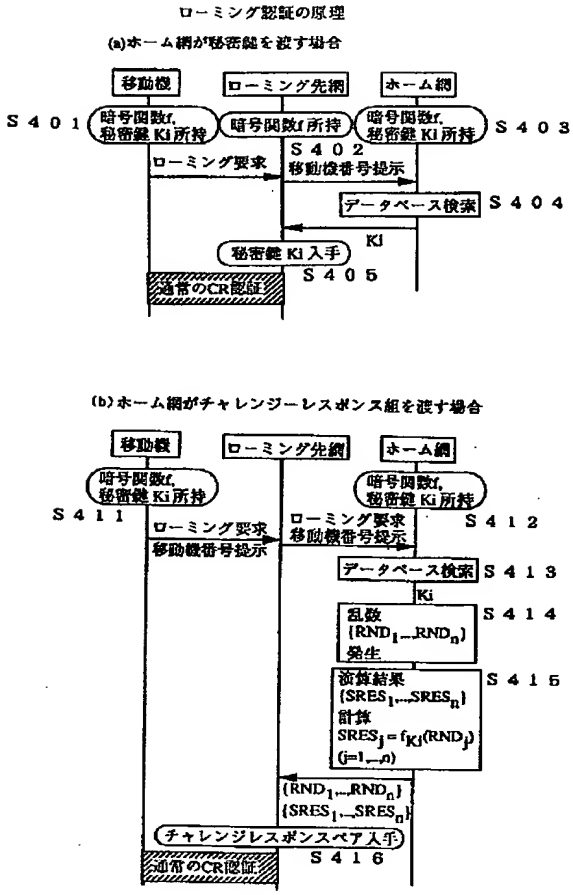
一括予備認証後の本認証



【図３】



【図４】



フロントページの続き

(51) Int. Cl.[6]	識別記号	庁内整理番号	F I	技術表示箇所
Ｈ０４Ｑ　7/34				
			Ｈ０４Ｑ　7/04	Ｃ

(72)発明者　山口　明
東京都新宿区西新宿２丁目３番２号国際電信電話株式会社内

(72)発明者　酒井　清一郎
東京都新宿区西新宿２丁目３番２号国際電信電話株式会社内

(72)発明者　水野　俊夫
東京都新宿区西新宿２丁目３番２号国際電信電話株式会社内